 2.2.1

Director of Central Intelligence
Security Committee
Computer Security Subcommittee

21 May 1985
DCISEC-CSS-M173

The one hundred and seventy-third meeting of the DCI SECOM Computer Security Subcommittee was held on 21 May 1985 at the STAT [redacted] McLean, VA. Present at the meeting were the following:

STAT [redacted] DIA, Chairman
Maj Jack Freeman, Army
Mr. Carl Martz, Navy
Mr. Norm Clark, Navy
Ms. Martha Toffer, Air Force
STAT [redacted] NSA
STAT [redacted] CIA
Mr. Lynn McNulty, State Department
STAT [redacted] SECOM
STAT [redacted] IC Staff

1. The first topic was a presentation by Carl Martz of the Navy's project on collection requirements for determining the Soviet threat to U.S. classified computer systems and data bases. Mr. Martz plans to give this briefing at the SECOM meeting next week; both as a status report and to support continued funding by SECOM. While this project has not produced any "smoking guns" to support the threat assessment, it has revealed that pertinent information is not contained in the available Intelligence STAT Reports because the desired information in not being asked [redacted] STAT [redacted] There was some follow on discussion about the focus of this particular project and its relationship with other threat studies being conducted within the Community. STAT [redacted] was asked to track this project with the SECOM.

2. The second topic was an update of three major efforts of the I. C. Staff's Computer Security Project: a threat and vulnerabilities study, safeguards, and a technology assessment. STAT [redacted] talked about the recently published threat report which used all sources input from throughout the Community. The attempt was to quantify the threat and they found 37 independent incidents (sorted out from over 500 reports) of the rising interests of hostile intelligence. The report concentrates on vulnerabilities of the I. C. systems or systems that process S.I. data. It provides a comprehensive coverage and a fairly accurate assessment of the threats and vulnerabilities; but the threat is still weak because "we don't know what we don't know".

The development of the Safeguards resulted from a need for a basis for evaluating the vulnerabilities of a select subset of "critical systems" of the I. C. Two criteria for the safeguards were they must be achievable and affordable. Initially there were 41 safeguards composed of 21 requirements from the "B 2"

level of the DoD Computer Security Evaluation Criteria (Orange Book), and 20 non-technical requirements for administrative procedures, physical protection, etc. The current version of the Safeguards contains only 29 of these, mostly non-technical, since many of the "B 2" level were not considered to be doable as a result of the assessment of the "critical systems" against the initial set of safeguards. The major weaknesses found in the "critical systems" were that they had not been accredited, lacked adequate accountability features, and that the physical security
STAT was weak. [redacted] stated that the DCI would like all new systems to meet the Safeguards, as a minimum.

STAT [redacted] chaired a Technology Assessment Working Group as part of the I. C. project to determine what was available in the market place today. Their report along with the Threat Study and Safeguards document was distributed to the NFIC and the NSDD-145 Steering Group. As regards funding, only the upgrading of the I. C. Staff's critical system was supported. Dollars for the remainder of the upgrades has been put back into
STAT the FY-86 budget requests. [redacted] pointed out that Mr. Latham, ASDC3I, has asked both DIA and NSA to assess how the implementation of the Safeguards would impact DoD systems across the board. The DCI is being asked to implement the Safeguards; i.e, fix the critical systems, by the end of FY-86.

3. The next topic for discussion was the development of policy and guidance for Personal Computer (PC) security. Mr.
STAT [redacted] and [redacted] reported on the three planning meetings held with Dennis Steinhauer, from National Bureau of Standards. These meetings have also included members of the DoD Computer Security Center, who are working on a similar effort, in order to assure consistency of policy or guidance across the various communities of interest. It is the intent of the Subcommittee to contract with NBS for this effort; NBS has already published a general PC security guide for management and developed PC guidance for State Department. The subcommittee members were shown a proposed layout for a foldout which would highlight some key PC security "dos and don'ts", which could be completed for distribution in the near time frame. Mr. Steinhauer had also prepared a first draft of a detailed outline of a user's guide for PC security which was provided to the members for comment. Two other levels of guidance, management and technical, are also being proposed. The first of these documents would probably not be ready before the end of the year. It was noted by Mr.
STAT [redacted] that the Standards Working Group of the Subcommitte for Automated Information Systems Security (SAISS) under NSDD-145 was also pursuing a similar effort. The Subcommittee agreed to
STAT continue the planned contract with NBS; [redacted] will follow up
STAT on the funding arrangements, and [redacted] will follow up on the SAISS effort to assure there is no duplication of effort.

4. The last item of discussion was the problems associated with the co-utilization of computer systems by various members of the I.C. or compartmented programs at contractor facilities. There does not appear to be adequate guidance as to assignment of

responsibilities for accrediting such systems. Currently, CIA has Memorandum of Understanding with several contractors and the other Community users of shared computer facilities; but they do not believe it is appropriate nor practical for them to assume the accreditation responsibility in all cases, particularly when they are a minor user of the system or are not privileged to have access to information about the other usage of the shared systems. Additional discusssion of this topic revealed that the clarification of accreditation responsibility was broader than just the co-utilization of the computer systems, i.e., extended to the whole facility, and should probably be passed along to the Subcommittee for Compartmentation for their consideration and
STAT resolution. [redacted] was asked to raise this issue with the
STAT SECOM Chairman; [redacted] and [redacted] agreed to help him to
STAT formulate the issue. [redacted] also pointed out we should consider an addendum to DCID 1/16 to address the issue of MOU's for assignment of responsibility when there are multiple Community users of computer systems and networks. The current draft revision to DCID 1/16 contains a section on this which could be used for such an addendum.

5. There being no further business, the meeting was adjourned at 1215. The next meeting was set for 0930 on 18 June
STAT at [redacted] McLean, VA.

STAT [redacted]

Executive Secretary